(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
6. Februar 2003 (06.02.2003)

PCT

(10) Internationale Veröffentlichungsnummer
WO 03/010638 A1

(51) Internationale Patentklassifikation[7]: G06F 1/00, G07F 7/10, G06F 9/318, 11/16

(21) Internationales Aktenzeichen: PCT/EP02/07298

(22) Internationales Anmeldedatum:
2. Juli 2002 (02.07.2002)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
101 36 335.4 26. Juli 2001 (26.07.2001) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **INFINEON TECHNOLOGIES AG** [DE/DE]; St.-Martin-Str. 53, 81669 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **JANKE, Marcus** [DE/DE]; Spitzingplatz 3, 81539 München (DE). **LAACKMANN, Peter** [DE/DE]; Schlierseestr. 11, 81541 München (DE).

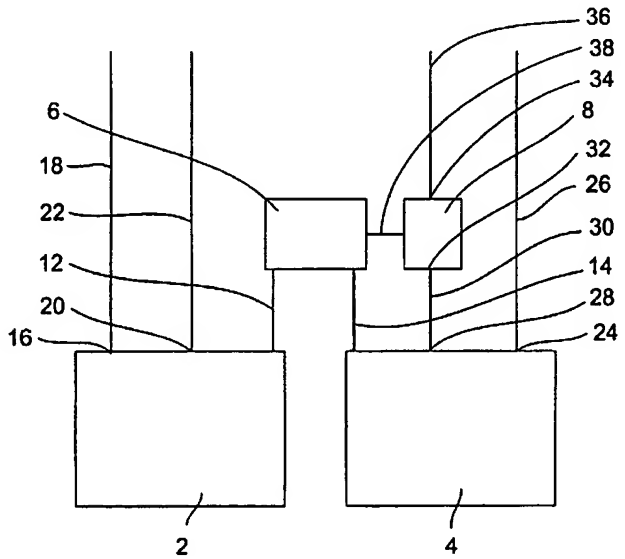
(74) Anwälte: **SCHOPPE, Fritz** usw.; SCHOPPE, ZIMMERMANN, STÖCKELER & ZINKLER, POSTFACH 71 08 67, 81458 München (DE).

(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

[Fortsetzung auf der nächsten Seite]

(54) Title: PROCESSOR COMPRISING A NUMBER OF ARITHMETIC-LOGIC UNITS

(54) Bezeichnung: PROZESSOR MIT MEHREREN RECHENWERKEN



(57) Abstract: The invention relates to a processor comprising a first arithmetic-logic unit (2), a second arithmetic-logic unit (4) and a control device (6) for controlling both arithmetic-logic units (2, 4). The control device controls the arithmetic-logic units in such a manner that they operate, as desired, in a high-security operational mode, in which complementary data is processed, or in a parallel operational mode, in which independent data is processed, or in a security operational mode, in which the same the data is processed, or are located in a power saving mode, in which one of the arithmetic-logic units (2, 4) is switched off.

[Fortsetzung auf der nächsten Seite]

WO 03/010638 A1

(84) **Bestimmungsstaaten** *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *mit internationalem Recherchenbericht*

— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Prozessor mit mehreren RechenwerkenEin Prozessor umfaßt ein erstes Rechenwerk (2), ein zweites Rechenwerk (4) und eine Steuereinrichtung (6) zum Ansteuern der beiden Rechenwerke (2, 4) derart, daß diese wahlweise in einer komplementäre Daten verarbeitenden Hochsicherheitsbetriebsart oder in einer unabhängige Daten verarbeitenden Parallelbetriebsart oder in einer gleiche Daten verarbeitenden Sicherheitsbetriebsart arbeiten oder sich in einer Leistungssparbetriebsart befinden, in der eines der Rechenwerke (2, 4) abgeschaltet ist.

Beschreibung

Prozessor mit mehreren Rechenwerken

Die vorliegende Erfindung bezieht sich auf einen Prozessor mit mehreren Rechenwerken und insbesondere auf einen Prozessor mit mehreren Rechenwerken, die in einer wählbaren Betriebsart entsprechend der Dual-Rail-Logik zusammenwirken können.

Mikroprozessoren bzw. Controller für Chipkartenanwendungen und andere kryptographische Anwendungen müssen häufig besonderen Sicherheitsbedingungen genügen. Eine der Hauptanforderungen ist die Sicherheit des Mikroprozessors gegen ein unberechtigtes Auslesen geheimer Informationen, insbesondere über Seitenkanalangriffe ("side channel attacks"). Seitenkanalangriffe erfolgen beispielsweise durch eine Erfassung der Leistungsaufnahme eines Prozessors oder über eine elektromagnetische oder elektrostatische Erfassung von Signalflüssen, wobei aus den so gewonnenen Informationen Rückschlüsse auf interne Vorgänge in dem Prozessor gezogen werden können. Neben Hochsicherheitsaufgaben muß ein Chipkartencontroller aber auch eine Vielzahl konventioneller Operationen ausführen, bei denen eine hohe Leistung einen großen Vorteil darstellt und einen wichtigen Marktvorteil ergeben kann. Als Beispiele wären hier Anwendungen aus dem Mobilfunkbereich zu nennen, bei denen die eigentliche Authentikation nur einen sehr geringen Teil der Programmlaufzeit ausmacht. Trotzdem wird für diesen geringen Anteil die volle Sicherheit der Authentikation verlangt. Ähnliches gilt auch für elektronische Geldbörsen, sogar für die Geldkarte, denn auch bei diesen Anwendungen sind große Teile des Programmablaufs wenig sicherheitskritisch, die eigentliche Authentikation ist jedoch eine Hochsicherheitsaufgabe.

Eine hochsichere Ausführung des Prozessorkerns ist z. B. in der sog. Dual-Rail-Logik mit Precharge möglich. Die Ausfüh-

rung eines Sicherheitsmikrocontrollers in Dual-Rail-Logik mit Precharge ist eine wichtige Maßnahme gegen Seitenkanalangriffe, die heute eine große Bedrohung darstellen. Sie verursacht jedoch einen im Vergleich zu einem herkömmlichen Prozessor wirtschaftlich nachteiligen größeren Flächenbedarf und kann durch die Notwendigkeit mehrerer Taktphasen zu Leistungseinbußen des Mikroprozessors führen. Dies hat im Vergleich zu Standardarchitekturen eine geringere Rechenleistung bzw. einen geringen Datendurchsatz sowie einen erhöhten Leistungsbedarf des Prozessors zur Folge.

Die Aufgabe der vorliegenden Erfindung besteht darin, einen Prozessor mit erhöhter Sicherheit zu schaffen, der eine höhere Rechenleistung bzw. einen kleineren Leistungsbedarf aufweist.

Diese Aufgabe wird durch einen Prozessor gemäß Anspruch 1, 2, 3 oder 11 gelöst.

Ein Prozessor gemäß der vorliegenden Erfindung umfaßt ein erstes Rechenwerk, ein zweites Rechenwerk und eine Steuereinrichtung zum Ansteuern der beiden Rechenwerke derart, daß diese wahlweise in einer komplementäre Daten verarbeitenden Hochsicherheitsbetriebsart oder in einer unabhängige Daten verarbeitenden Parallelbetriebsart arbeiten. Anstatt der Parallelbetriebsart oder zusätzlich kann als weitere Betriebsart eine Leistungssparbetriebsart, in der eines der Rechenwerke abgeschaltet ist, oder eine Sicherheitsbetriebsart, in der beide Rechenwerke parallel gleiche Daten verarbeiten, vorgesehen sein.

Gemäß einem bevorzugten Ausführungsbeispiel der vorliegenden Erfindung umfaßt ein Prozessor ferner eine schaltbare Komplementierungseinrichtung mit einem Ausgang, der mit einem Eingang des zweiten Rechenwerks verbunden ist, zum Empfangen von Daten und zum wahlweisen Ausgeben der empfangenen Daten oder des Komplements der empfangenen Daten.

Ein Prozessor gemäß der vorliegenden Erfindung kann ferner ein drittes Rechenwerk und ein viertes Rechenwerk umfassen, wobei das dritte Rechenwerk und das vierte Rechenwerk durch die Steuereinrichtung derart ansteuerbar sind, daß sie wahlweise in einer komplementäre Daten verarbeitenden Hochsicherheitsbetriebsart oder in einer unabhängige Daten verarbeitenden Parallelbetriebsart arbeiten. In einer anstelle der Hochsicherheitsbetriebsart oder zusätzlich zu ihr vorgesehenen Leistungssparbetriebsart ist das dritte und/oder das vierte Rechenwerk abgeschaltet.

Das erste Rechenwerk und das zweite Rechenwerk sind vorzugsweise derart ausgestaltet, daß sie in der Hochsicherheitsbetriebsart zeitsynchron die gleichen Befehle verarbeiten können. Das erste Rechenwerk und das zweite Rechenwerk sind vorzugsweise räumlich benachbart angeordnet. Der Prozessor kann beispielsweise ein Kryptographieprozessor sein.

Ein weiterer Prozessor gemäß der vorliegenden Erfindung umfaßt ein erstes Rechenwerk, ein zweites Rechenwerk, eine Datenquelle, welche mit dem ersten Rechenwerk und dem zweiten Rechenwerk derart verbunden ist, daß synchron dem ersten Rechenwerk Daten und dem zweiten Rechenwerk das Komplement der Daten zugeführt werden, und eine Befehlsquelle, welche ein Paar von Befehlen aufweist, wobei einer der Befehle des Befehlspaares für das erste Rechenwerk vorgesehen ist und wobei der andere Befehl des Befehlspaares für das zweite Rechenwerk vorgesehen ist, und wobei die Befehlsquelle mit dem ersten Rechenwerk und dem zweiten Rechenwerk derart verbunden ist, daß synchron der für das erste Rechenwerk vorgesehene Befehl des Befehlspaares dem ersten Rechenwerk und der für das zweite Rechenwerk vorgesehene Befehl des Befehlspaares dem zweiten Rechenwerk zugeführt werden können.

Der für das erste Rechenwerk vorgesehene Befehl und der für das zweite Rechenwerk vorgesehene Befehl können gleich sein,

wenn der Prozessor in einer Dual-Rail-Betriebsart oder einer Sicherheitsbetriebsart arbeiten soll, sie können voneinander verschieden sein, wenn der Prozessor in einer Hochleistungsbetriebsart arbeiten soll, und einer der beiden Befehle kann das Rechenwerk, für das er vorgesehen ist, stillegen, wenn der Prozessor in einer Leistungssparbetriebsart arbeiten soll.

Eine weitere Aufgabe der vorliegenden Erfindung besteht darin, eine Chipkarte mit erhöhter Sicherheit und einer verbesserten Rechenleistung und/oder einem verringerten Leistungsbedarf zu schaffen.

Diese Aufgabe wird durch eine Chipkarte gemäß Anspruch 13 gelöst.

Eine Chipkarte gemäß der vorliegenden Erfindung umfaßt einen der oben beschriebenen Prozessoren.

Der vorliegenden Erfindung liegt die Erkenntnis zugrunde, daß eine Dual-Rail-Logik durch eine Anordnung mehrerer Prozessorteilmodule realisiert werden kann, die in verschiedenen Betriebsarten betrieben werden können. Vorteilhaft enthält ein solcher Mikroprozessor zwei oder eine andere gerade Anzahl von CPU-Teilmodulen, die zumindest paarweise identisch aufgebaut sind. Bei zwei CPU-Teilen kann zwischen vier verschiedenen Betriebszuständen gewählt und im Betrieb umgeschaltet werden:

1. Hochsicherheitsbetriebsart: Einer der beiden CPU-Teile bzw. eines der beiden Rechenwerke arbeitet wie ein herkömmlicher Standardprozessor. Der zweite Teil jedoch wird mit den komplementären Daten versorgt und bearbeitet diese zeitsynchron mit exakt den gleichen Befehlen und der gleichen Ansteuerung, wobei die Rechenwerke im Precharge-Betrieb arbeiten. Damit wirken die beiden Prozessorteile zusammen wie ein einziger Prozessor mit Du-

al-Rail-Logik, sie befinden sich in der Hochsicherheitsbetriebsart. Vorteilhaft sind die komplementär rechnenden Elemente räumlich nebeneinander angeordnet und vorzugsweise sind sie ferner verwoben angeordnet, wodurch eine solche Anordnung auch gegen elektromagnetische Abstrahlungsanalysen gesichert werden kann. Im Sinne dieser Anmeldung ist ein Prozessor mit komplementär rechnende Rechenwerke ein Prozessor mit einer von verarbeiteten Daten unabhängigen Stromaufnahme.

2. Hochleistungsbetriebsart: Für Programme oder Programmteile, bei denen eine starke Sicherung gegen Seitenkanalangriffe nicht erforderlich ist, ist die Hochleistungsbetriebsart vorgesehen. In dieser Betriebsart werden die CPU-Teile bzw. Rechenwerke mit parallel abzuarbeitenden bzw. unterschiedlichen Programmteilen versorgt. So entsteht eine Anordnung von zwei CPUs bzw. Prozessoren, wodurch sich der Datendurchsatz verdoppeln kann.

3. Leistungssparbetriebsart: In der Leistungssparbetriebsart wird eines oder mehrere Rechenwerke deaktiviert, so daß nur noch ein Rechenwerk oder ein Teil der Rechenwerke arbeitet. Durch die kleinere Anzahl von schaltenden Gattern ist die Leistungsaufnahme reduziert. Der Prozessor arbeitet in dieser Betriebsart weder im Bereich der höchsten Sicherheitsstufe noch im Bereich der höchsten Leistung.

4. Sicherheitsbetriebsart: Eine Sicherheitsbetriebsart ist eine Betriebsart, bei der zwei Rechenwerke die gleichen Daten verarbeiten und durch Vergleich der Ergebnisse dieser Verarbeitung die Betriebssicherheit erhöht wird, was beispielsweise einen Schutz gegen DFA (differential fault attack) bietet.

Ein Vorteil des erfindungsgemäßen Prozessors besteht darin, daß er die hohe Sicherheit einer Dual-Rail-Logik für sicherheitsrelevante Programme bzw. Programmteile und eine hohe Rechenleistung oder einen geringeren Leistungsbedarf für eine Verarbeitung weniger sicherheitsrelevanter Programmteile bietet, wobei zwischen verschiedenen Betriebsarten dynamisch auch während des Betriebes geschalten werden kann.

Wenn in der vorliegenden Anmeldung von zwei Rechenwerken die Rede ist, können jeweils $n \cdot 2$ Rechenwerke zum Einsatz kommen, wobei n eine natürliche Zahl ist.

Ein bevorzugtes Ausführungsbeispiel der vorliegenden Erfindung wird nachfolgend Bezug nehmend auf die beiliegenden Zeichnungen näher erläutert. Es zeigen:

Fig. 1 eine schematische Darstellung eines Ausführungsbeispiels der vorliegenden Erfindung;

Fig. 2 eine schematische Darstellung einer Hochsicherheitsbetriebsart des Ausführungsbeispiels aus Fig. 1;

Fig. 3 eine schematische Darstellung einer Hochleistungsbetriebsart des Ausführungsbeispiels aus Fig. 1;

Fig. 4 eine schematische Darstellung einer Leistungssparbetriebsart des Ausführungsbeispiels aus Fig. 1; und

Fig. 5 eine schematische Darstellung einer Sicherheitsbetriebsart des Ausführungsbeispiels aus Fig. 1.

Fig. 1 ist eine schematische Darstellung des für die vorliegende Erfindung relevanten Teils eines Prozessors gemäß einem Ausführungsbeispiel der vorliegenden Erfindung. Der Prozessor weist ein erstes Rechenwerk 2, ein zweites Rechenwerk 4, eine

Steuereinrichtung 6 und eine Komplementierungseinrichtung 8 auf. Im Fall von zwei parallelen Datenleitungen kann die Komplementierungseinrichtung 8 durch einen Inverter gebildet sein. Die Steuereinrichtung 6 ist mit dem ersten Rechenwerk 2 über eine Steuerleitung 12 und mit dem zweiten Rechenwerk 4 über eine Steuerleitung 14 wirksam verbunden. Das erste Rechenwerk 2 weist einen Befehlseingang 16, der über eine Leitung 18 mit einer nicht dargestellten Befehlsquelle, beispielsweise einem Programmspeicher in Form eines ROMs (ROM = Read Only Memory = Nur-Lese-Speicher), eines RAMs (RAM = Random Access Memory = Speicher mit wahlfreiem Zugriff) oder einer Festplatte, verbunden ist, sowie einen Dateneingang 20, der über eine Datenleitung 22 mit einer nicht dargestellten Datenquelle, beispielsweise einem Datenspeicher oder einer Schnittstelle verbunden ist, auf. Das zweite Rechenwerk 4 weist einen Befehlseingang 24, der über eine Befehlsleitung 26 mit der nicht dargestellten Befehlsquelle, mit der das erste Rechenwerk über die Befehlsleitung 18 verbunden ist, oder mit einer anderen Befehlsquelle verbunden ist, und einen Dateneingang 28, der über eine Datenleitung 30 mit einem Ausgang 32 der Komplementierungseinrichtung 8 verbunden ist, auf. Die Komplementierungseinrichtung 8 weist ferner einen Eingang 34 auf, der über eine Datenleitung 36 mit der Datenquelle, mit der das erste Rechenwerk 2 über die Datenleitung 22 verbunden ist, oder einer anderen Datenquelle verbunden ist. Die Steuereinrichtung 6 und die Komplementierungseinrichtung 8 sind über eine Steuerleitung 38 wirksam verbunden.

Das erste Rechenwerk 2 bzw. das zweite Rechenwerk 4 verarbeitet gesteuert durch Befehle, die ihm an dem Befehlseingang 16 bzw. 24 zugeleitet werden, Daten, die ihm am Dateneingang 20 bzw. 28 zugeleitet werden. Die Komplementierungseinrichtung 8 ist steuerbar bzw. schaltbar, d. h. sie gibt an ihrem Ausgang 32 wahlweise Daten aus, die sie am Eingang 34 empfangen hat (Komplementierungseinrichtung ausgeschaltet) oder deren Komplement (Komplementierungseinrichtung eingeschaltet). Diese beiden Zustände der Komplementierungseinrichtung 8 werden

durch die Steuereinrichtung 6 über die Steuerleitung 38 gesteuert bzw. geschaltet. Die Steuereinrichtung 6 steuert ferner das erste Rechenwerk 2 und das zweite Rechenwerk 4 um mehrere verschiedene Betriebsmodi bzw. Betriebsarten einzustellen, die nachfolgend anhand der Fig. 2 bis 4 näher beschrieben werden.

Fig. 2 ist eine schematische Darstellung einer Hochsicherheitsbetriebsart des Ausführungsbeispiels aus Fig. 1. In dieser Betriebsart empfangen das erste Rechenwerk 2 und das zweite Rechenwerk 4 an dem Befehlseingang 16 bzw. 24 dieselben Befehle zur Verarbeitung von Daten. Ferner werden dem ersten Rechenwerk 1 am Dateneingang 20 und der Komplementierungseinrichtung 8 am Eingang 34 dieselben Daten zugeleitet. Die Komplementierungseinrichtung 8 ist eingeschaltet, d. h. sie gibt am Ausgang 32 das Komplement der Daten aus, die sie am Eingang 34 empfängt. Das zweite Rechenwerk 4 empfängt somit an seinem Dateneingang 28 das Komplement der Daten, die das erste Rechenwerk 2 an seinem Dateneingang 20 empfängt. In dieser Hochsicherheitsbetriebsart entspricht die Funktion des Prozessors gemäß dem vorliegenden Ausführungsbeispiel somit der Dual-Rail-Logik, d. h. die vorzugsweise baugleichen Rechenwerke 2 und 4 verarbeiten gesteuert durch dieselben Befehle synchron komplementäre Daten. In dieser Hochsicherheitsbetriebsart ist ein Seitenkanalangriff über eine Messung der Leistungsaufnahme des Prozessors stark erschwert oder gar unmöglich, da die Leistungsaufnahme des ersten Rechenwerks und des zweiten Rechenwerks zusammen aufgrund der Verarbeitung komplementärer Daten nicht von den Daten abhängig ist. Wenn das erste Rechenwerk 2 und das zweite Rechenwerk 4 in räumlicher Nähe zueinander oder ineinander verwoben angeordnet werden, wird ferner ein Seitenkanalangriff über eine Analyse der elektromagnetischen Abstrahlung des Prozessors wesentlich erschwert, da aufgrund der Verarbeitung komplementärer Daten immer in unmittelbarer Nähe zueinander Ströme bzw. Spannungen auftreten, welche einem digitalen Wert und seinem Komplement entsprechen.

Fig. 3 zeigt eine Hochleistungsbetriebsart des ersten Rechenwerks 2 und des zweiten Rechenwerks 4. In dieser Betriebsart werden dem ersten Rechenwerk 2 und dem zweiten Rechenwerk 4 an ihren Dateneingängen 20 und 28 verschiedene Daten und an ihren Befehlseingängen 16 und 24 verschiedene Befehle zugeführt. Durch die parallele bzw. gleichzeitige Verarbeitung verschiedener oder gleicher Daten mit verschiedenen oder gleichen Befehlen bzw. Programmen oder Programmteilen verdoppelt sich die Rechenleistung des Prozessors gemäß dem vorliegenden Ausführungsbeispiel. Der Prozessor kann somit in der gleichen Zeit und mit der gleichen Leistungsaufnahme wie in der Hochsicherheitsbetriebsart, gesteuert durch die doppelte Anzahl von Befehlen, die doppelte Anzahl von Daten verarbeiten. Gleichzeitig bietet diese Betriebsart aber nicht den besonderen Schutz gegen Seitenkanalangriffe, den die anhand der Fig. 2 erläuterte Hochsicherheitsbetriebsart bietet. Sie bietet jedoch den Vorteil der Verschleierung der Stromprofile sowie der elektromagnetischen Abstrahlung durch parallele Verarbeitung verschiedener Daten.

Fig. 4 ist eine schematische Darstellung einer Leistungssparbetriebsart. In dieser Betriebsart ist eines der beiden Rechenwerke, hier das zweite Rechenwerk 4, abgeschaltet bzw. es wird nicht mit Leistung versorgt. Das andere Rechenwerk, hier das erste Rechenwerk 2, empfängt Daten und Befehle, welche es verarbeitet. In dieser Betriebsart sind die Leistungsaufnahme und die Rechenleistung der beiden Rechenwerke gegenüber der anhand Fig. 3 erläuterten Hochleistungsbetriebsart halbiert. Wie die Hochleistungsbetriebsart bietet auch die Leistungssparbetriebsart nicht die besondere Sicherheit gegenüber Seitenkanalangriffen, welche die anhand der Fig. 2 erläuterte Hochsicherheitsbetriebsart bietet.

Fig. 5 ist eine schematische Darstellung einer Sicherheitsbetriebsart des Ausführungsbeispieles aus Fig. 1. In dieser Betriebsart empfangen das erste Rechenwerk 2 und das zweite Re-

chenwerk 4 an dem Befehlseingang 16 bzw. 24 dieselben Befehle zur Verarbeitung von Daten. Ferner werden dem ersten Rechenwerk 1 am Dateneingang 20 und der Komplementierungseinrichtung 8 am Eingang 34 dieselben Daten zugeleitet. Die Komplementierungseinrichtung 8 ist ausgeschaltet, d. h. sie gibt am Ausgang 32 die Daten aus, die sie am Eingang 34 empfängt. Das zweite Rechenwerk 4 empfängt somit an seinem Dateneingang 28 die gleichen Daten, die das erste Rechenwerk 2 an seinem Dateneingang 20 empfängt. In dieser Sicherheitsbetriebsart verarbeiten das erste Rechenwerk 2 und das zweite Rechenwerk 4 gesteuert durch dieselben Befehle synchron die gleichen Daten. Die durch beide Rechenwerke ausgegebenen Ergebnisse werden einer in Fig. 1 nicht dargestellten Vergleichseinrichtung zugeführt, welche die Ausgabe des ersten Rechenwerkes 2 und die Ausgabe des zweiten Rechenwerkes 4 auf Übereinstimmung überprüft und abhängig davon ein Signal ausgibt, welches verwendet werden kann, um beispielsweise eine Wiederholung der Verarbeitung der Eingangsdaten, eine Verwendung von Defaultdaten bzw. voreingestellten Daten anstelle der ausgegebenen Ergebnisse, eine Plausibilitätsüberprüfung der beiden ausgegebenen Ergebnisse, eine vorübergehende Unterbrechung oder einen vollständigen Abbruch der Datenverarbeitung durch die Rechenwerke oder eine andere voreingestellte Reaktion zu steuern bzw. auszulösen. Dadurch bietet die Sicherheitsbetriebsart einen Schutz gegen einen DFA.

Entsprechend kann auch bei der oben anhand der Fig. 2 dargestellten Hochsicherheitsbetriebsart eine Überprüfung der durch das erste Rechenwerk 2 und das zweite Rechenwerk 4 ausgegebenen Ergebnisse auf Komplementarität durchgeführt werden.

Die anhand der Fig. 2 bis 5 erläuterten Betriebsarten eignen sich für verschiedene Aufgaben, welche ein Prozessor, beispielsweise ein Prozessor in einer Chipkarte oder ein anderer Kryptoprozessor oft abwechselnd oder nacheinander erfüllen muß. Bei der Abarbeitung von Programmen oder Programmteilen

zur Authentikation, zur Verschlüsselung oder zum Zugriffsschutz ist eine maximale Sicherheit gegenüber Angriffen Unbefugter, beispielsweise gegenüber Seitenkanalangriffen, erforderlich. Der Umfang dieser extrem sicherheitsrelevanten Aufgaben ist dabei oft vergleichsweise gering. Sie werden in der Hochsicherheitsbetriebsart ausgeführt, welche eine maximale Sicherheit und eine mittlere Leistung bietet.

Den größten Umfang haben bei vielen Anwendungen Operationen bzw. Aufgaben des Prozessors, die geringere oder gar keine Anforderungen an die Sicherheit gegenüber Angriffen stellen, deren Abarbeitung in möglichst kurzer Zeit jedoch erwünscht ist, beispielsweise um einem Anwender einen hohen Komfort zu bieten und ihm Wartezeiten zu ersparen. Diese Operationen können in der Hochleistungsbetriebsart ausgeführt werden, die einen geringeren Grad an Sicherheit gegenüber Angriffen, aber eine im Vergleich zur Hochsicherheitsbetriebsart verdoppelte Rechenleistung bietet.

Ferner treten bei zahlreichen Anwendungen Aufgaben auf, bei denen nur eine geringe oder fast verschwindende Rechenleistung erforderlich ist, weil beispielsweise im Programmablauf auf eine Eingabe eines Anwenders oder eine Information, die von einer anderen Einrichtung angefordert wurde, gewartet wird. Diese Aufgaben können in der Leistungssparbetriebsart ausgeführt werden, welche die geringe Rechenleistung der Hochsicherheitsbetriebsart mit der geringen Sicherheit der Hochleistungsbetriebsart kombiniert, dabei aber den Leistungsbedarf der Rechenwerke halbiert.

Ein Vorteil eines Prozessors gemäß der vorliegenden Erfindung besteht darin, daß durch eine Realisierung von zwei oder drei der oben beschriebenen Betriebsarten, insbesondere der Hochsicherheitsbetriebsart zusammen mit der Hochleistungsbetriebsart und/oder der Leistungssparbetriebsart, eine flexible Anpassung von Sicherheitsstandard, Rechenleistung und Leistungsbedarf möglich ist, wobei zwischen den Betriebsarten

dynamisch bzw. während des Betriebs umgeschaltet bzw. gewechselt werden kann. So kann beispielsweise in der Hochleistungsbetriebsart ein Anwender aufgefordert werden, eine PIN einzugeben, in der Leistungssparbetriebsart auf eine Eingabe der PIN gewartet werden und diese anschließend in der Hochsicherheitsbetriebsart kryptographisch verarbeitet werden.

Zur Realisierung eines Prozessors, der gemäß der vorliegenden Erfindung zwei, drei oder vier der anhand der Fig. 2 bis 5 erläuterten Betriebsarten aufweist, ist die in Fig. 1 schematisch dargestellte Schaltung aus dem ersten Rechenwerk 2, dem zweiten Rechenwerk 4, der Steuereinrichtung 6 und der Komplementierungseinrichtung 8 nur ein Beispiel. Alternativ zu der Darstellung in Fig. 1 kann beispielsweise die Komplementierungseinrichtung 8 ein Bestandteil des zweiten Rechenwerks 4 und dessen Dateneingang 28 nachgeschaltet sein und/oder es kann eine weitere Komplementierungseinrichtung in der Datenleitung 22 des ersten Rechenwerks oder im ersten Rechenwerk 2 vorgesehen sein. Abhängig von der Architektur bzw. der verwendeten Schaltung der Rechenwerke 2 und 4 kann ferner unter Umständen auf eine Komplementierungseinrichtung verzichtet werden, weil beispielsweise zum Komplementieren lediglich zwei Leitungen gekreuzt werden müssen.

Die Steuereinrichtung 6 kann das erste Rechenwerk 2 und das zweite Rechenwerk 4 durch die Steuerleitungen 12 und 14 anschalten bzw. aktivieren und (in der Leistungssparbetriebsart) ausschalten bzw. stillegen, sie kann dies alternativ aber auch über einen Zugriff auf die Leistungsversorgung der beiden Rechenwerke tun.

Eine Zuführung derselben Daten über die Datenleitung 22 an den Dateneingang 20 des ersten Rechenwerks 2 und über die Datenleitung 36 an den Eingang 34 der Komplementierungseinrichtung 8 ist auf verschiedene Weisen möglich. Beispielsweise können durch eine in Fig. 1 nicht dargestellte "Datenweiche", die mit den Datenleitungen 22 und 36 verbunden ist, Daten von

einer Datenquelle synchron zum Dateneingang 20 des ersten Rechenwerks 2 und zum Eingang 34 in der Komplementierungseinrichtung 8 geleitet werden.

Alternativ kann eine Datenweiche in die Steuereinrichtung 6 integriert sein. Dann ist abweichend von der Darstellung in Fig. 1 die Steuereinrichtung 6 mit einer Datenquelle verbunden, wobei der Dateneingang 20 des ersten Rechenwerks 2 über eine Datenleitung mit der Steuereinrichtung 6 verbunden ist, und wobei der Eingang 34 der Komplementierungseinrichtung 8 über eine Datenleitung mit der Steuereinrichtung 6 verbunden ist. Die Steuereinrichtung 6 kann dann je nach der erwünschten Betriebsart dieselben Daten synchron zu dem ersten Rechenwerk 2 und über die komplementierende oder nicht komplementierende Komplementierungseinrichtung 8 zu dem zweiten Rechenwerk 4 leiten oder verschiedene Daten an das erste Rechenwerk 2 und über die nicht-komplementierende Komplementierungseinrichtung 8 an das zweite Rechenwerk 4 leiten oder nur Daten an das erste Rechenwerk 2 leiten.

Auch beim Leiten von Befehlen über die Befehlsleitungen 18 und 26 an den Befehlseingang 16 des ersten Rechenwerks 2 bzw. den Befehlseingang 24 des zweiten Rechenwerks 4 existieren verschiedene Möglichkeiten. Der Befehlseingang 16 des ersten Rechenwerks 2 und der Befehlseingang 24 des zweiten Rechenwerks 4 können über die Befehlsleitungen 18 bzw. 26 direkt mit ein und derselben oder mit zwei verschiedenen Befehlsquellen verbunden sein, wie es oben in Zusammenhang mit Fig. 1 erläutert wurde. Alternativ kann eine Befehlsquelle mit der Steuereinrichtung 6 verbunden sein, welche über eine Befehlsleitung mit dem Befehlseingang 16 des ersten Rechenwerks und über eine Befehlsleitung mit dem Befehlseingang 24 des zweiten Rechenwerks verbunden ist. Die Steuereinrichtung 6 leitet dann je nach der erwünschten Betriebsart synchron dieselben Befehle oder verschiedene Befehle an den Befehlseingang 16 des ersten Rechenwerks 2 und den Befehlseingang 24 des zwei-

ten Rechenwerks 4 oder aber nur an eines der beiden Rechenwerke 2 und 4.

Die Steuereinrichtung 6 zum Ansteuern der beiden Rechenwerke 2 und 4 kann also auf verschiedene Weise ausgeführt und mit dem ersten Rechenwerk 2, dem zweiten Rechenwerk 4 und der Komplementierungseinrichtung 8 wirksam verbunden sein, damit in Abhängigkeit von der erwünschten Betriebsart das erste Rechenwerk 2 und das zweite Rechenwerk 4 synchron dieselben oder verschiedene Daten und Befehle verarbeiten können oder damit eines der beiden Rechenwerke 2 und 4 stillgelegt werden kann.

Ferner ist eine Software-Realisierung der oben anhand der Fig. 2 bis 4 erläuterten Betriebsarten und des Wechsels zwischen denselben möglich. In diesem Fall weist der Prozessor ein erstes Rechenwerk 2 und ein zweites Rechenwerk 4 auf, und die Steuereinrichtung ist durch Befehle realisiert, welche durch den Prozessor bzw. die Rechenwerke ausführbar sind. Der Befehlseingang 16 des ersten Rechenwerks 2 und der Befehlseingang 24 des zweiten Rechenwerks 4 sind mit einer Befehlsquelle bzw. einem Programmspeicher, beispielsweise einem ROM (ROM = read only memory = Nur-Lese-Speicher), verbunden. Das erste Rechenwerk 2 und das zweite Rechenwerk 4 weisen jeweils einen oder mehrere Dateneingänge 20 bzw. 28 auf, wobei alle Datenquellen, welche Daten liefern, die in der Hochsicherheitsbetriebsart verarbeitet werden sollen, beispielsweise eine Anwenderschnittstelle, über die von einem Anwender eine PIN eingegeben wird, parallel so mit einem Dateneingang 20 des ersten Rechenwerks und einem Dateneingang 28 des zweiten Rechenwerks verbunden sind, daß dem ersten Rechenwerk 2 die Daten der Datenquelle und synchron dazu dem zweiten Rechenwerk 4 das Komplement der Daten der Datenquelle zugeleitet werden.

Dies kann, wie es bereits oben anhand des in Fig. 1 dargestellten Ausführungsbeispiels erläutert wurde, beispielsweise

durch eine Komplementierungseinrichtung in der Datenleitung zwischen der Datenquelle und dem Dateneingang des zweiten Rechenwerks oder aber, je nach der verwendeten Architektur der Rechenwerke, auch durch einfaches Kreuzen von Datenleitungen erfolgen. Die Befehlsquelle enthält Paare von Befehlen, wobei jeweils einer der Befehle für das erste Rechenwerk vorgesehen ist und diesem über einem Befehlseingang 16 zugeführt wird, und wobei der jeweils andere Befehl des Paars für das zweite Rechenwerk 4 vorgesehen ist, und diesem synchron über den Befehlseingang 24 zugeführt wird.

Programmteile, die für die oben anhand der Fig. 2 erläuterten Hochsicherheitsbetriebsart vorgesehen sind, weisen Paare von Befehlen auf, welche jeweils zwei identische Befehle umfassen. Programmteile, welche für eine Verarbeitung in der oben anhand der in Fig. 3 erläuterten Hochleistungsbetriebsart vorgesehen sind, weisen Befehlspaare auf, welche zwei gleichzeitig von dem ersten Rechenwerk 2 bzw. dem zweiten Rechenwerk 4 zu verarbeitende Befehle umfassen. Programmteile, welche für eine Verarbeitung in der oben anhand der Fig. 4 erläuterten Leistungssparbetriebsart vorgesehen sind, weisen Befehlspaare auf, welche für eines der Rechenwerke 2 und 4 einen auszuführenden Befehl und für das jeweils andere Rechenwerk einen nicht zu verarbeitenden Befehl oder einen Deaktivierungs- bzw. Abschaltbefehl aufweisen.

Bei Programmteilen, welche in der Hochsicherheitsbetriebsart ablaufen, verarbeiten somit das erste Rechenwerk 2 und das zweite Rechenwerk 4 gesteuert durch identische Befehle synchron komplementäre Daten von der gleichen Datenquelle. Bei Programmteilen, welche in der Hochleistungsbetriebsart ablaufen, verarbeiten das erste Rechenwerk 2 und das zweite Rechenwerk 4 gesteuert durch im allgemeinen voneinander verschiedene Befehle verschiedene Daten von ein und derselben oder verschiedenen Datenquellen. Bei Programmteilen, welche für eine Bearbeitung in der Leistungssparbetriebsart vorgesehen sind, bearbeitet eines der beiden Rechenwerke gesteuert

durch Befehle Daten und das andere Rechenwerk ist stillgelegt bzw. abgeschaltet. Im Fall von drei oder mehr Rechenwerken ist eine Kombination der Betriebsmodi möglich.

Die oben dargestellten Ausführungsbeispiele sind ohne weiteres auf Prozessoren mit mehr als zwei Rechenwerken, vorzugsweise mit einer geraden Anzahl von paarweise baugleichen Rechenwerken erweiterbar. In diesem Fall können alle Paare von Rechenwerken in derselben Betriebsart oder aber in verschiedenen Betriebsarten arbeiten. In der Leistungssparbetriebsart können alle Rechenwerke bis auf eines abgeschaltet sein. Im Fall von drei oder mehr Rechenwerken ist eine Kombination der Betriebsarten möglich.

Die vorliegende Erfindung eignet sich für alle Prozessoren, welche für kryptographische Anwendungen oder Sicherheitsanwendungen verwendet werden können und vor Seitenkanalangriffen geschützt werden sollen, beispielsweise für Prozessoren in Chipkarten.

Bezugszeichenliste

2	erstes Rechenwerk
4	zweites Rechenwerk
6	Steuereinrichtung
8	Invertiereinrichtung
12	Steuerleitung
14	Steuerleitung
16	Befehlseingang
18	Befehlsleitung
20	Dateneingang
22	Datenleitung
24	Befehlseingang
26	Befehlsleitung
28	Dateneingang
30	Datenleitung
32	Ausgang der Invertiereinrichtung
34	Eingang der Invertiereinrichtung
36	Datenleitung
38	Steuerleitung

Patentansprüche

1. Prozessor mit folgenden Merkmalen:

einem ersten Rechenwerk (2);

einem zweiten Rechenwerk (4); und

einer Steuereinrichtung (6) zum Ansteuern der beiden Rechenwerke (2) und (4) derart, daß diese wahlweise in einer komplementäre Daten verarbeitenden Hochsicherheitsbetriebsart oder in einer unabhängige Daten verarbeitenden Parallelbetriebsart arbeiten.

2. Prozessor mit folgenden Merkmalen:

einem ersten Rechenwerk (2);

einem zweiten Rechenwerk (4); und

einer Steuereinrichtung (6) zum Ansteuern der beiden Rechenwerke (2) und (4) derart, daß diese wahlweise in einer komplementäre Daten verarbeitenden Hochsicherheitsbetriebsart arbeiten oder sich in einer Leistungssparbetriebsart befinden, in der eines der Rechenwerke (2, 4) abgeschaltet ist.

3. Prozessor mit folgenden Merkmalen:

einem ersten Rechenwerk (2);

einem zweiten Rechenwerk (4); und

einer Steuereinrichtung (6) zum Ansteuern der beiden Rechenwerke (2) und (4) derart, daß diese wahlweise in einer komplementäre Daten verarbeitenden Hochsicherheitsbetriebsart oder in einer gleiche Daten verarbeitenden Sicherheitsbetriebsart arbeiten.

4. Prozessor gemäß einem der Ansprüche 1 bis3, ferner mit einer schaltbaren Komplementierungseinrichtung (8), mit einem Ausgang (32), der mit einem Eingang (28) des zweiten Rechenwerks (4) verbunden ist, zum Empfangen von Daten und zum wahlweisen Ausgeben der empfangenen Daten oder des Komplements der empfangenen Daten.

5. Prozessor gemäß einem der Ansprüche 1 bis 4, ferner mit folgenden Merkmalen:

einem dritten Rechenwerk; und

einem vierten Rechenwerk;

wobei das dritte Rechenwerk und das vierte Rechenwerk durch die Steuereinrichtung (6) derart ansteuerbar sind, daß sie wahlweise in einer komplementäre Daten verarbeitenden Hochsicherheitsbetriebsart oder in einer unabhängige Daten verarbeitenden Parallelbetriebsart arbeiten.

6. Prozessor gemäß einem der Ansprüche 1 bis 4, ferner mit folgenden Merkmalen:

einem dritten Rechenwerk; und

einem vierten Rechenwerk;

wobei das dritte Rechenwerk und das vierte Rechenwerk durch die Steuereinrichtung (6) derart ansteuerbar sind, daß sie wahlweise in einer komplementäre Daten verarbeitenden Hochsicherheitsbetriebsart arbeiten oder sich in einer Leistungssparbetriebsart befinden, in der das dritte und/oder das vierte Rechenwerk abgeschaltet ist.

7. Prozessor gemäß einem der Ansprüche 1 bis 4, ferner mit folgenden Merkmalen:

einem dritten Rechenwerk; und

einem vierten Rechenwerk;

wobei das dritte Rechenwerk und das vierte Rechenwerk durch die Steuereinrichtung (6) derart ansteuerbar sind, daß sie wahlweise in einer komplementäre Daten verarbeitenden Hochsicherheitsbetriebsart oder in einer gleiche Daten verarbeitenden Sicherheitsbetriebsart arbeiten.

8. Prozessor gemäß einem der Ansprüche 1 bis 7, bei dem das erste Rechenwerk (2) und das zweite Rechenwerk (4) derart ausgestaltet sind, daß sie in der Hochsicherheitsbetriebsart zeitsynchron die gleichen Befehle verarbeiten können.

9. Prozessor gemäß einem der Ansprüche 1 bis 8, bei dem das erste Rechenwerk (2) und das zweite Rechenwerk (4) räumlich benachbart oder ineinander verwoben angeordnet sind.

10. Prozessor gemäß einem der Ansprüche 1 bis 9, bei dem der Prozessor ein Kryptographie- oder Sicherheitsprozessor ist.

11. Prozessor mit folgenden Merkmalen:

einem ersten Rechenwerk (2);

einem zweiten Rechenwerk (4);

einer Datenquelle, welche mit dem ersten Rechenwerk (2) und dem zweiten Rechenwerk (4) derart verbunden ist, daß synchron dem ersten Rechenwerk (2) Daten und dem zweiten Rechenwerk (4) das Komplement der Daten zugeführt werden; und

einer Befehlsquelle, welche ein Paar von Befehlen aufweist, wobei einer der Befehle des Befehlspaares für das erste Rechenwerk (2) vorgesehen ist und wobei der andere Befehl des

Befehlspaares für das zweite Rechenwerk (4) vorgesehen ist, und die mit dem ersten Rechenwerk (2) und dem zweiten Rechenwerk (4) derart verbunden ist, daß synchron der für das erste Rechenwerk (2) vorgesehene Befehl des Befehlspaares dem ersten Rechenwerk (2) und der für das zweite Rechenwerk (4) vorgesehene Befehl des Befehlspaares dem zweiten Rechenwerk (4) zugeführt werden können.

12. Prozessor gemäß Anspruch 11, bei dem der für das erste Rechenwerk (2) vorgesehene Befehl und der für das zweite Rechenwerk (4) vorgesehene Befehl gleich sind.

13. Chipkarte mit einem Prozessor gemäß einem der Ansprüche 1 bis 12.

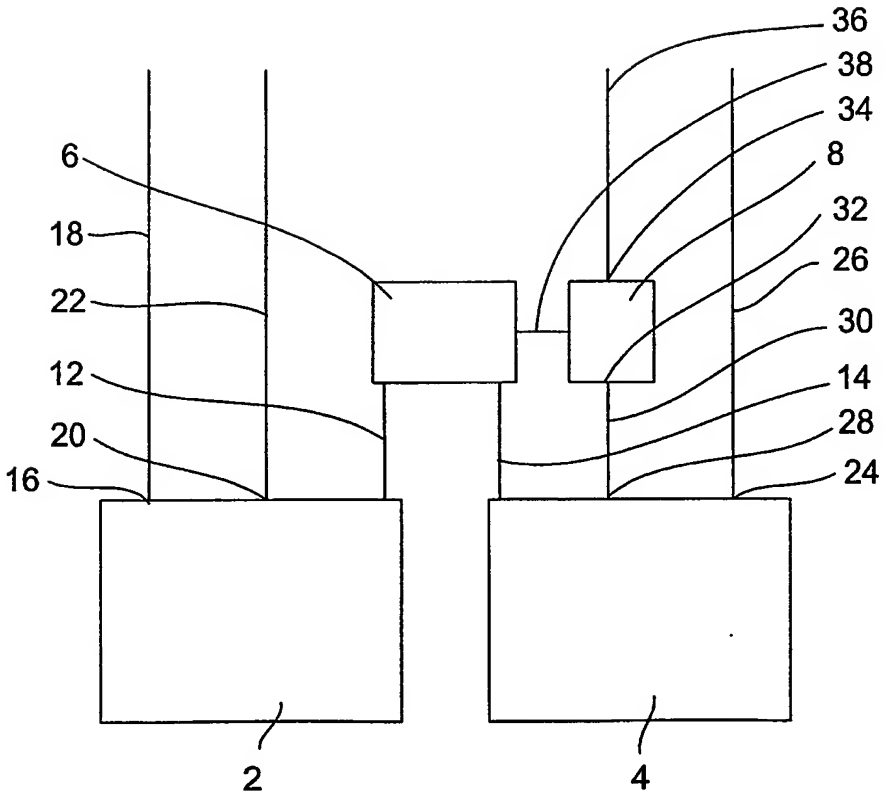


FIG 1

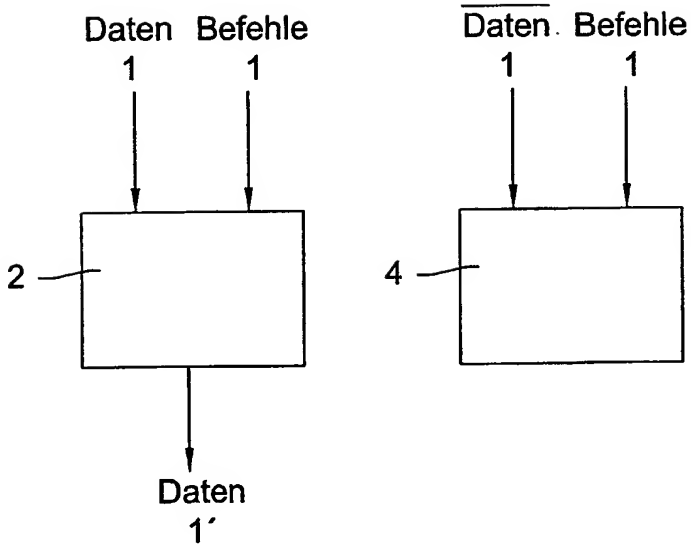


FIG 2

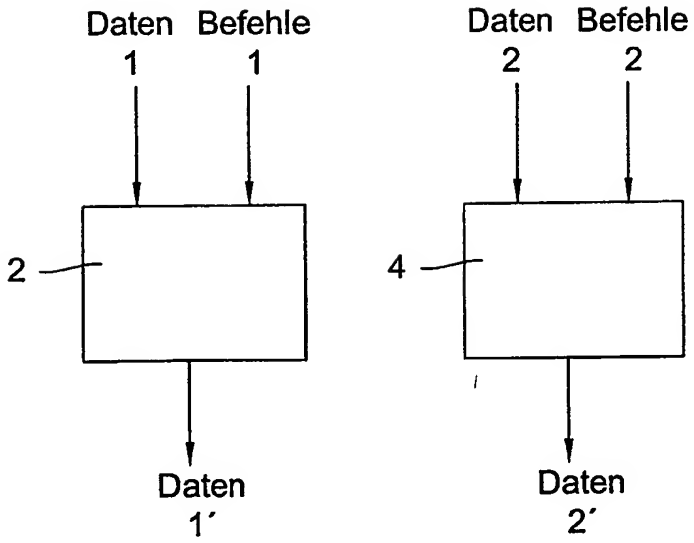


FIG 3

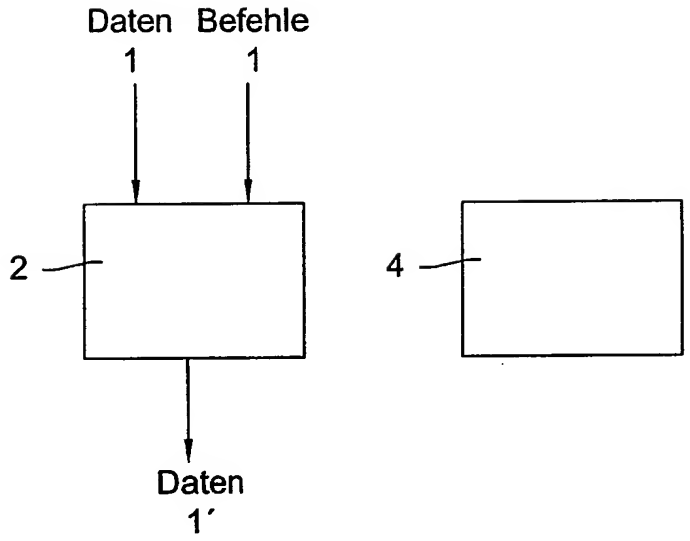


FIG 4

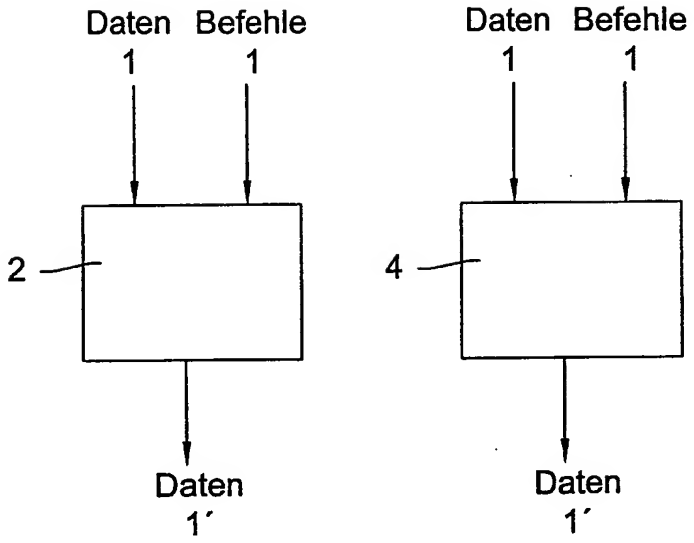


FIG 5

INTERNATIONAL SEARCH REPORT

Intel ›nal Application No
PCT/EP 02/07298

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 G07F7/10 G06F9/318 G06F11/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 1 115 094 A (PHILIPS CORP INTELLECTUAL PTY ;KONINKL PHILIPS ELECTRONICS NV (NL)) 11 July 2001 (2001-07-11) abstract; figure 1 column 6, line 20 -column 6, line 38 ---	1-13
Y	FR 2 787 900 A (BULL CP8) 30 June 2000 (2000-06-30) abstract; figures 3,4,6 page 11, line 11 -page 12, line 9 page 14, line 16 -page 15, line 4 page 17, line 1 -page 22, line 26 -----	1-13

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 November 2002	09/12/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Bozas, I

3

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

...ormation on patent family members

Inte onal Application No
PCT/EP 02/07298

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 1115094	A	11-07-2001	DE	10000503 A1	12-07-2001
			CN	1304116 A	18-07-2001
			EP	1115094 A2	11-07-2001
			JP	2001230771 A	24-08-2001
FR 2787900	A	30-06-2000	FR	2787900 A1	30-06-2000
			BR	9908268 A	24-10-2000
			CN	1292109 T	18-04-2001
			EP	1057094 A1	06-12-2000
			WO	0039660 A1	06-07-2000
			JP	2002533825 T	08-10-2002
			TW	463101 B	11-11-2001

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 02/07298

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F1/00 G07F7/10 G06F9/318 G06F11/16

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06F G07F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	EP 1 115 094 A (PHILIPS CORP INTELLECTUAL PTY ;KONINKL PHILIPS ELECTRONICS NV (NL)) 11. Juli 2001 (2001-07-11) Zusammenfassung; Abbildung 1 Spalte 6, Zeile 20 -Spalte 6, Zeile 38 ---	1-13
Y	FR 2 787 900 A (BULL CP8) 30. Juni 2000 (2000-06-30) Zusammenfassung; Abbildungen 3,4,6 Seite 11, Zeile 11 -Seite 12, Zeile 9 Seite 14, Zeile 16 -Seite 15, Zeile 4 Seite 17, Zeile 1 -Seite 22, Zeile 26 -----	1-13

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
28. November 2002	09/12/2002

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Bozas, I

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 02/07298

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
EP 1115094	A	11-07-2001	DE	10000503 A1	12-07-2001
			CN	1304116 A	18-07-2001
			EP	1115094 A2	11-07-2001
			JP	2001230771 A	24-08-2001
FR 2787900	A	30-06-2000	FR	2787900 A1	30-06-2000
			BR	9908268 A	24-10-2000
			CN	1292109 T	18-04-2001
			EP	1057094 A1	06-12-2000
			WO	0039660 A1	06-07-2000
			JP	2002533825 T	08-10-2002
			TW	463101 B	11-11-2001